What is claimed is:

1. A method of configuring a network security system, comprising:

a. forming a registry data structure for defining roles within a network;

b. mapping network security policies to the registry data structure, said network security policies being contained in one or more policy documents stored in machine readable form; and

c. using a document transformation algorithm to transform the policy documents into one or more device-specific configuration documents stored in machine-readable form.

2. The method according to claim 1, further comprising generating instances of the roles and associated security policies, each instance being mapped to physical segments of the network.

3. The method according to claim 1, further comprising distributing the device-specific configuration documents to network entities for implementing the network security policies.

4. The method according to claim 1, wherein the registry data structure comprises a collection of documents that include information regarding the network roles and topology of the network.

5. The method according to claim 1, wherein the registry data structure comprises a hierarchy of network types, each type comprising a definition of a network role.

6. The method according to claim 5, wherein each network role is representative of a set of applications to be supported by the network.

7. The method according to claim 5, wherein when a parent network type is mapped to a policy contained in one of the policy documents, a child network type of the parent network type inherits the policy.

8. The method according to claim 7, wherein when the child network type is mapped to a policy contained in one of the policy documents that is conflict with the policy inherited from the parent, the policy mapped to the child takes precedence over the policy inherited from the parent.

9. The method according to claim 5, wherein an instance of one of the network types is mapped to one or more physical network segments and wherein the network type includes a set of data fields for defining the physical network segments.

10. The method according to claim 6, wherein one of the network types is an abstract type without an instance mapped to a physical network segment.

11. The method according to claim 5, wherein each network type further comprises a data field for identifying a human administrator.

12. The method according to claim 5, wherein each network type further comprises a data field for providing a human readable description of the network type.

13. The method according to claim 1, wherein the network security policies are representative of restrictions to be placed on one or more of the network roles in the registry data structure.

14. The method according to claim 1, wherein the policy documents are in extensible markup language (XML).

15. The method according to claim 1, wherein the document transformation algorithm is specific to a network entity utilized for implementing one or more of the security policies contained in the policy documents.

16. The method according to claim 15, wherein the document transformation algorithm includes style sheet language for transformation (XSLT) controlled by a script.

17. The method according to claim 16, wherein the script is specific to a network entity.

18. The method according to claim 16, further comprising a step of selecting the script from among a plurality of scripts, each being specific to a different network entity.

19. The method according to claim 16, wherein the device-specific configuration documents are in plain text format.

20. A apparatus for configuring a network security system, comprising:

a. a registry data structure including a plurality of network types, each network type being stored within a document in the registry and including a role definition and a set of fields defining segments of a network;

b. security policy documents mapped to the registry data structure, each security policy document being representative of restrictions to be placed on a network type in the registry data structure; and

c. a document transformation algorithm for transforming the documents in the registry and the policy documents into device-specific configuration documents stored in machine-readable form.